# Exhibit B

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/387,711 | 03/13/2003 | Hamdy Soliman | NMTECH13 | 7643 |

30996 7590 07/02/2010

ROBERT W. BECKER & ASSOCIATES
707 HIGHWAY 333
SUITE B
TIJERAS, NM 87059-7507

| EXAMINER | |
|---|---|
| HENNING, MATTHEW T | |
| ART UNIT | PAPER NUMBER |
| 2431 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 07/02/2010 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

---

*Ex parte* HAMDY SOLIMAN

---

Appeal 2009-006119
Application 10/387,711
Technology Center 2400

---

Before LEE E. BARRETT, LANCE LEONARD BARRY, and HOWARD B. BLANKENSHIP, *Administrative Patent Judges*.

BARRY, *Administrative Patent Judge*.

DECISION ON APPEAL[1]

---

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

## STATEMENT OF THE CASE

The Patent Examiner rejected claims 1, 3, and 5-34. The Appellant appeals therefrom under 35 U.S.C. § 134(a). We have jurisdiction under 35 U.S.C. § 6(b).

## INVENTION

The Appellant describes the invention at issue on appeal as follows.

> A dynamic computer system security method and system using dynamic encryption and full synchronization between system nodes. A data record from a data stream created by a source user is encrypted with an initial dynamic session key. A new dynamic session key is generated based upon a data record and a previous dynamic session key. The new dynamic session key is then used to encrypt the next data record. A central authority is used to synchronize and authenticate both source and destination users with dynamic authentication keys. The central authority and users constantly regenerate new dynamic authentication keys.

(Spec. 35.)

## ILLUSTRATIVE CLAIMS

> 1. A method of providing a secure data stream between system nodes, the method comprising:
>
> providing a previous encryption key;
>
> creating a data record at a source node, the data record including plaintext to be exchanged;

regenerating a new encryption key at the source node as a function of the data record and a previous encryption key by performing a logic operation on the previous encryption key and the data record: and

performing a logic operation on the previous encryption key and the data record to form an expanded key.

18. A method of authenticating one system node to another system node, the method comprising the steps of:

generating an authentication key at a user node;

transmitting the authentication key to a central authority node; and

starting a daemon at each of the user node and the central authority node for continuously regenerating a new authentication key and maintaining a corresponding number-regeneration-counter at each of the user node and the central authority node.

## REJECTIONS

Claims 1, 3, and 5-17 stand rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 5,365,588 ("Bianco") and Applied Cryptography ("Schneier").

Claims 18-24 and 27-29 stand rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 6,839,434 ("Mizikovsky") and U.S. Patent Application No. 2003/0217292 ("Steiger").

Claim 25 stands rejected under 35 U.S.C. § 103(a) as unpatentable over Mizikovsky; Steiger; and U.S. Patent No. 5,253,294 ("Maurer").

Claim 26 stands rejected under 35 U.S.C. § 103(a) as unpatentable over Mizikovsky; Steiger; Maurer; and U.S. Patent No. 6,301,664 ("Di-Crescenzo").

Claims 30 and 33 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Mizikovsky; Steiger; and Operating System Concepts ("Silberschatz").

Claims 31, 32, and 34 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Mizikovsky; Steiger; Silberschatz and Handbook of Applied Cryptography ("Menezes").

## CLAIMS 1, 3, AND 5-17

The Examiner finds that "Schneier teaches that in one known method of key generation, called cipher-feedback mode, the plaintext input is encrypted with the 'previous encryption key', and the encrypted text is then fed back into the key generation (See Schneier Page 200) . . . ." (Answer 4.) The Appellant argues that "Schneier cannot be used to support a finding of obviousness with respect to claim 1 because the teachings of Schneier are antithetical to the recitations of claim 1." (Reply Br. 9.) Therefore, the issue before us is whether the Examiner erred in finding that the combined teachings of Bianco and Schneier would have suggested regenerating a new encryption key at a source node as a function of a plaintext record and a previous encryption key by performing a logic operation on the previous encryption key and the plaintext as required by claim 1.

## FINDINGS OF FACT

Bianco "relates to general purpose, high speed encryption algorithms." (Col. 1, ll. 6-7.)

The page of Schneier cited by the Examiner teaches that "[b]lock ciphers can also be implemented as a self-synchronizing stream cipher; this is called cipher-feedback (CFB) mode." (p. 200.)

## ANALYSIS

"The Patent and Trademark Office (PTO) must consider all claim limitations when determining patentability of an invention over the prior art." *In re Lowry*, 32 F.3d 1579, 1582 (Fed. Cir. 1994) (citing *In re Gulack*, 703 F.2d 1381, 1385 (Fed. Cir. 1983)). Here, considering all the limitations of independent claim 1, we agree with the Appellant's following construction of the claim.

> As clearly reflected in the language of claim 1, the data record itself includes the plaintext to be exchanged, from which one can readily infer that the step of regenerating the encryption key is a function of a previous encryption key and, by substitution of terms, the plaintext to be exchanged.

(Reply Br. 8.)

The question of obviousness is "based on underlying factual determinations including . . . what th[e] prior art teaches explicitly and inherently . . . ." *In re Zurko*, 258 F.3d 1379, 1383 (Fed. Cir. 2001). Here, the Examiner admits that "Bianco did not specifically disclose regenerating a new encryption key as a function of the data record and a previous encryption key by performing a logic operation on the previous encryption key and the data record." (Answer 4.) Because Bianco does not regenerate a new encryption key at a source node as a function of *any* data record, the same reference does not regenerate a new encryption key at a source node as a function of a *plaintext* record.

Turning to the second reference, we agree with the Examiner's aforementioned finding that Schneier teaches that in the cipher-feedback mode encrypted text is fed back into the key generation. The Examiner concludes that "[i]t would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the encryption system of Bianco by feeding back the encrypted output into the working register" (Answer 4) of the latter reference. Assuming *arguendo* that such a modification would have been obvious and that the result would have been operable, we are unpersuaded that the result would have suggested the contested limitations of claim 1. To the contrary, we find that the proposed modification would have regenerated a new encryption key at a source node as a function of a *ciphertext* record and a previous encryption key by performing a logic operation on the previous encryption key and the *ciphertext*.

Based on the aforementioned facts and analysis, we conclude that the Examiner erred in finding that the combined teachings of Bianco and Schneier would have suggested regenerating a new encryption key at a source node as a function of a plaintext record and a previous encryption key by performing a logic operation on the previous encryption key and the plaintext as required by claim 1 and claims 3 and 5-17, which depend therefrom.

CLAIMS 18-33

Based on the Appellant's arguments, we will decide the appeal of claims 18-33 based on claim 18 alone. The Examiner finds that Mizikovsky teaches all of the limitations of claim 18 including that "[c]ol. 8 Lines 38-39

of Mizikovsky discloses that the procedure of Mizikovsky, which includes the generation of SSD [i.e., shared secret data key], is carried out periodically, which falls within the scope of continuously." (Answer 18.) He recognizes that the reference "does not specifically call his SSD generation procedure a daemon." (*Id.*) The Examiner offers two explanations to cure the omission.

The first explanation, which comprises several findings, follows.

> [A] daemon, quite simply, is a program that performs a housekeeping or maintenance utility function without being called by the user. The periodicity of Mizikovsky is not due to the procedure being called by a user, as can be seen in Col. 8 Lines 38-45. Further, reauthentication and regeneration of SSD falls within the scope of a maintenance function. As such, the SSD generation procedure of Mizikovsky basically reads on the definition of a daemon.

(*Id.*)

The second explanation, which comprises a finding and a conclusion, follows.

> Steiger teaches that in a key updating system, a daemon should be run on each of the nodes for maintaining the synchronization of the keys (See Steiger Paragraph 0051).
>
> It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Steiger in the periodic key updating system by running a daemon on each node to perform the regenerating/ synchronization.

(*Id.* at 7.)

The Appellant argues that "Steiger . . . does not teach or disclose the use of daemons for regenerating authentication keys between a user node and a central authority node." (App. Br. 11.) Therefore, the issue before us is

whether the Examiner erred in finding that the combined teachings of Mizikovsky and Steiger, in combination with the knowledge of persons skilled in the art, would have suggested using daemons to regenerate authentication keys between a user node and a central authority node.

## FINDINGS OF FACT

Mizikovsky "relates to . . . the updating of keys or other information used by communicating parties." (Col. 1, ll. 8-10.) More specifically, the reference "shows an embodiment of the key update and bidirectional validation procedure between a wireless unit and the wireless communications system." (Col. 7, ll. 5-7.) The key that is updated is referred to as "a shared key (SSD)." (*Id.* at l. 9.)

Steiger "relates generally to network security . . . ." (¶ [0002], ll. 1-2.) More specifically, the latter reference teaches that a "gatekeeper 430 may take the form of a daemon operating on each of a plurality of import servers 112 and serve to keep key information stored locally up to date and substantially synchronized with other import servers 112." (¶ [0051], ll. 1-4.)

## ANALYSIS

"Non-obviousness cannot be established by attacking references individually where the rejection is based upon the teachings of a combination of references." *In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986) (citing *Keller*, 642 F.2d at 425). "The test for obviousness is what the combined teachings of the references would have suggested to one of

ordinary skill in the art." *In re Young*, 927 F.2d 588, 591 (Fed. Cir. 1991) (citing *In re Keller*, 642 F.2d 413, 425 (CCPA 1981)).

In determining obviousness, furthermore, a reference "must be read, not in isolation, but for what it fairly teaches in combination with the prior art as a whole." *Id.* "'Every patent application and reference relies to some extent upon knowledge of persons skilled in the art to complement that [which is] disclosed . . . .'" *In re Bode*, 550 F.2d 656, 660 (CCPA 1977) (quoting *In re Wiggins*, 488 F.2d 538, 543 (CCPA 1973)). Those persons "must be presumed to know something" about the art "apart from what the references disclose." *In re Jacoby*, 309 F.2d 513, 516 (CCPA 1962).

Here, the Examiner's aforementioned finding that Mizikovsky teaches continuously regenerating authentication keys between a user node and a central authority node is uncontested. "Silence implies assent." *Harper & Row Publishers, Inc. v. Nation Enters.,* 471 U.S. 539, 572 (1985). His first explanation, *supra*, is also uncontested. For our part, we agree with the Examiner that persons skilled in the art would have known that a daemon is a program that performs a housekeeping or maintenance utility function without being called by the user. We also agree with him that column 8, lines 38-45, of Mizikovsky supports his finding that the periodicity of the reference's reauthentication is not based on manual activation. We agree with the Examiner that Mizikovsky's reauthentication and regeneration of its SSD key falls within the scope of a maintenance function. Therefore, we agree with him that the reference's regeneration of its SSD is performed by a daemon. The Appellant does not address, let alone show error in, these findings.

Second, the rejection is based on the combined teachings of Mizikovsky and Steiger. As mentioned previously, the Examiner's finding that Mizikovsky teaches continuously regenerating authentication keys between a user node and a central authority node is uncontested. The Appellant admits that "Steiger discloses the use of one or more daemons to provide key maintenance at one or more import servers . . . ." (App. Br. 11.) Therefore, we are persuaded that the combined teachings of Mizikovsky and Steiger would have suggested using daemons to regenerate authentication keys between a user node and a central authority node. Based on the aforementioned facts and analysis, we conclude that the Examiner did not err in finding that the combined teachings of Mizikovsky and Steiger, in combination with the knowledge of persons skilled in the art, would have suggested using daemons to regenerate authentication keys between a user node and a central authority node.

CLAIM 34

The Examiner finds that "Mizikovsky further disclosed generating an authentication key (SSD) based upon a previous authentication key (RANDSSD)." (Ans. 20.) Besides reiterating the argument made for claims 18-33, the Appellant argues that "Menenzes does not teach or disclose the step of regenerating an authentication key based on a previous authentication key at both the central authority node and the user node." (App. Br. 17.) Therefore, the issue before us is whether the Examiner erred in finding that the combined teachings of Mizikovsky and Steiger, in combination with the knowledge of persons skilled in the art, would have

suggested regenerating an authentication key based on a previous authentication key at both a central authority node and a user node.

## ANALYSIS

The rejection is based on the combined teachings of Mizikovsky, Steiger, Silberschatz, and Menezes. As mentioned regarding claims 18-33, the Examiner's finding that Mizikovsky teaches continuously regenerating authentication keys between a user node and a central authority node is uncontested. Likewise, his additional finding that "Mizikovsky further disclosed generating an authentication key (SSD) based upon a previous authentication key (RANDSSD)" (Ans. 20) is also uncontested. The Appellant cannot establish non-obviousness by attacking Menezes individually as lacking a limitation that the Examiner relies on Mizikovsky to teach. Based on the aforementioned facts and analysis, we conclude that the Examiner did not err in finding that the combined teachings of Mizikovsky and Steiger, in combination with the knowledge of persons skilled in the art, would have suggested regenerating an authentication key based on a previous authentication key at both a central authority node and a user node.

## DECISION

We reverse the rejection of claims 1, 3, and 5-17. In contrast, we affirm the rejections of claims 18-34.

No time for taking any action connected with this appeal may be extended under 37 C.F.R. § 1.136(a)(1). *See* 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED-IN-PART

rwk

ROBERT W. BECKER & ASSOCIATES
707 HIGHWAY 333
SUITE B
TIJERAS NM 87059-7507